Briefing paper on the telecoms package and a copyright enforcement policy frameworkDRAFT
Written by Monica Horten
University of Westminster, Communications and Media Research Insitute
PhD research: The Political Battle for Online Content in the European Union
09.11.2008

Packaging up copyright enforcement

- how the Telecoms Package slots in the framework for a European policy to restrict Internet content

Abstract
This paper discusses how certain amendments to a review of European telecoms law, known as the Telecoms Package, will establish the foundations for an EU-wide policy framework that supports the enforcement of copyright on the Internet. Arguably, it also opens the door to widespread surveillance and filtering of Internet content, and limitations on users' rights to access and distribute content. It is being slipped in via a series of amendments, disguised in legal text that deliberately obscures their true intent, with very little opposition in the EU legislature - and bypassing the established EU policy processes and scrutiny.

Hotly debated and controversial in the European Parliament, the copyright amendments overshadowed the review's true objectives on internal market and competition policy. And yet, there is a sense in which they have become the elephant in the room, the topic that is delicately avoided, away from the heated corridors of the rue Wiertz.

The Telcoms Package, in its latest draft[i], will impose on national telecoms regulators an obligation to protect copyrighted content. Regulators will also have an obligation to pursue a policy of copyright enforcement, expressed in the law as the "*promoting co-operation*" between ISPs and "*the sectors interested in the promotion of lawful content*".

It will enable member states to legislate for mechanisms to such as the French graduated response or 3-strikes. It will pile on the pressure to ISPs to filter, "throttle" and block Internet content, especially peer-to-peer file sharing, by creating legal work-arounds to undermine the mere conduit status which currently exonerates ISPs from liability for content.

In this context, the user's right to a contract which specifies restrictions on access to content, services and applications, becomes a poisoned chalice – something which seems very good, but in fact harms the person it is given to - because it is also the same mechanism which gives ISPs the right to filter content or cut off users who infringe copyright.

Copyright enforcement measures arguably undermine certain fundamental rights of European citizens. Safeguards which protect users against abusive practices or false allegations risk being weakened, whether they take the form of regulatory oversight, privacy rules, or due process.

However, copyright enforcement measures are also criticised for imposing a potentially damaging liability burden on the Internet industry, which is expected to carry Europe into the next era of the Information Society.

See also **Annexe: Analysis of certain amendments in the Telecoms Package in respect of a copyright enforcement policy framework**

Written by Monica Horten
University of Westminster, Communications and Media Research Insitute
PhD research: The Political Battle for Online Content in the European Union
09.11.2008

Packaging up copyright enforcement

- how the Telecoms Package slots in the framework for a European policy to restrict Internet content

The review of European telecommunications law, known as the Telecoms Package, is currently passing through the EU legislature. It has become controversial due to amendments related to copyright enforcement on the Internet, which were inserted in the committee stages of its progress through the European Parliament. The controversy around these amendments has hi-jacked the debate and the real purpose of the review, which was intended to deal with internal market and competition issues for the telecoms industry. Arguably, they have put the entire review into jeopardy[ii].

These amendments, which support the requirement that telecoms regulators must '*promote the co-operation*'between network operators and "*the sectors interested in the promotion of lawful content"* embed within the telecoms framework law an obligation on regulators to protect copyrighted content on the Internet – an obligation which they will have to pass on to the network operators and Internet service providers (ISPs)[iii].

Taken individually, the amendments do not mandate any explicit measures for copyright enforcement. But when analysed together, the amendments put in place a foundation stone for online copyright enforcement enabling the sanctioning of users at the say-so of copyright owners, and the filtering and blocking of audio-visual, music and broadcast content. It is argued that they point to an outcome of widespread surveillance of Internet users[iv].

The matter is problematic because the amendments are written in opaque language, and placed in different parts of five directives, so that they are difficult to find. Indeed after some adverse publicity just before the European Parliament committee vote on July 7th, there has been more effort to hide the meaning, using even more vague language. It has become the elephant in the room, unavoidable, but the EU public relations material does not discuss it.

The Telecoms Package amendments are controversial because the economic stakes are high. There is a sense in which the debate around the Telecoms Package exemplifies the strained relationship between copyright as a mechanism for economic value on the one hand, and the individual right to freedom of expression and privacy on the other[v]. The debate is highly polarised, and broadly speaking puts the Internet industry and digital rights campaigners in one camp and the content producers and collecting societies (rights-holders) in the other.

The overt issue is the widespread availability of 'free' content on the Internet, and the future funding of the content industries. If Internet content is available for free for users to download, commercial content producers argue that they derive no return on their investment, and the value of content products is eroded. The underlying issue is the consequent loss of freedom of users to access content, services and applications, and the implications, both social and economic, of surveillance in support of copyright.

.

The economic problem of downloading[vi] is about large numbers of people – millions of Internet users – taking files of music, film and broadcast content from file-sharing sites, or uploading it onto their own pages on websites, and thereby committing small-scale infringements of copyright – using copyrighted material without payment and without the relevant permission from the author or rights-holder. The rights-holders refer to it as 'mass-scale' infringement[vii] and campaign at a political level in a variety of policy fora[viii].

They argue for measures which aim to deal with large numbers of people, committing potentially very small offences, in the electronic environment. However, their main target in 2008 is the people who download via peer-to-peer filesharing sites. The measures they want include graduated response (a series of warnings followed by termination of Internet access); electronic fingerprinting and tracking of content, filtering and blocking, both at the end –users computer on and on the network.

The measures they argue for have been devised in order to get around certain legal barriers. European data protection law, intended to safeguard user's privacy, is from the rights-holder perspective, is one such barrier[ix]. The only way they can legally get into direct contact with the end-user is via the ISP[x].

This means the rights-holders can't do it on their own. They need the help – "co-operation" of the Internet industry. But this raised another issue: the E-commerce directive, which enshrines a principle of "mere conduit" exonerating the ISPs from liability for Internet content, and has enabled the ISPs to successfully argue against any "co-operation" for copyright enforcement. "Mere conduit" was a barrier that, from the rights-holder perspective, they had to get around before the ISPs would "co-operate". They have been campaigning since 2006 for the EU to "*remedy the anachronistic nature of the regulatory framework*" and for a regulatory "*nudge*" towards increased "*co-operation*" which should facilitate among other things, "*means of redress to victims of civil wrongs*" and "*the take-up and use of technological tools discouraging or preventing illegal activities*"[xi].

Most of the policy options for copyright enforcement relate in some way to altering the liability of the Internet service provider in order to undermine the "mere conduit" principle and this is where I believe the heat of fire in this battle is burning. By finding a way to make the ISPs liable for content, they are put into a position of having to enforce it. Effectively, we are talking about some form of secondary liability. The pressure is currently very heavy for ISPs to address the key target of peer-to-peer, where the only option for them is to use an automated, technological, blocking tool.

Copyright enforcement in Europe

The European Union has no policy on copyright enforcement in respect of the specific issues related to Internet downloading, other than that which is set out in the 2001 Copyright Directive[xii] and in the 2004 IPR Enforcement Directive[xiii]. The measures in both directives require measures to be proportionate, equitable and applied under due process of law.

However, the downloading of Internet content, especially of music, presents a different problem from that envisaged in either of these Directives. The IPR Enforcement directive is intended to deal with commercial-scale infringements and not individual users infringing for their own use. Therefore it is not suitable to deal with the problem of downloading Internet content and there has been pressure from the rights-holder industries to create new legal devices to deal with it.

There is a policy process to determine what the EU policy on copyright enforcement should be. It is taking place within the European Commission, which was consulting on it[xiv]. There has been no policy decision taken, and the Commission has not yet come out with any policy proposals.

The only previous decision that was taken at a political level was taken by the European Parliament on 9th April 2008, when it voted for an amendment to the Bono report with a large majority[xv]. This amendment positively rejected the concept of graduated response, making a clear statement that graduated response is an unacceptable policy in the EU. Amendments attempting to insert the rights-holders demands into the Bono report had previously been rejected by the Culture committee[xvi].

Rights-holders lobbied for a legal obligation at EU level for ISPs to work with them - "co-operate" - on copyright enforcement. They had made it clear that this is what they wanted to see in the Telecoms Package when it was unveiled by the European Commission in November 2007. What they wanted was a way around the 'mere conduit' principle.

There is no doubt as to the intent. Shortly before the unveiling, there were media reports touting the inclusion of '*droit d'auteur*'. It was reported to be driven by the Information Society Commissioner, Viviane Reding, herself, who believed that at a time of technological convergence, it was appropriate to apply regulation which obliged telecoms operators to fight against online piracy[xvii]. Two amendments hooking in copyright, were inserted after the draft left the responsible team at DG Information Society, by the College of Commissioners. The rest were inserted *ad hoc* in the committee stages of the European Parliament.

The Telecoms Package

Thus the amendments which placed copyright enforcement into the Telecoms Package are not part of any agreed EU policy. As is now publicly stated by the MEP Ruth Hieronymi,[xviii] they were inserted by MEPs who support the rights-holder lobby, and want 'stronger protection of copyright and neighbouring rights' for online content.

What we are seeing with the Telecoms Package, is policy for copyright enforcement being made 'on the fly' by lawyers advising lobbyists, who pass texts to MEPs. Whilst it is normal for amendment in the European Parliament committees to alter legislation, it is not normal for the amendments to extend the *scope* of legislation, in the way that these amendments extend the scope of telecommunications law, from regulating electronic transmission to regulating online content.

It is a policy which is little understood, partly due to the rushed nature of the process, and partly due to the way the amendments are being inserted into different parts of the different directives, only making sense when someone is able to link them together[xix]. It has wide societal and economic implicatons which are not receiving the legislative scrutiny that they deserve.

The French presidency is pushing for the Telecoms Package to be passed by the end of the year[xx], before it hands over to the Czech government, and its passage through the European Parliament has, for this reason, been rushed. Many of these amendments were passed in the committee vote on July 7th. The plenary vote on 24 September added some amendments which safeguarded users rights (see Annexe). At the time of writing, these amendments risk being deleted by the Council of Ministers.

This raises a number of very important policy considerations for European policy makers.

The policy framework for online copyright enforcement

The policy framework for online copyright enforcement, using civil law, offers three possible alternative approaches[xxi]. The first deals with users directly, by implementing civil law sanctions – an example is graduated response, where the ultimate sanction for users who infringe copyright is to cut off their Internet access. However, as cutting off Internet access has been widely condemned, an alternative being considered is to use technical, automated measures[xxii] – this is what is generally referred to as filtering. The third approach is indirect, and less well understood, but it entails putting pressure on Internet Service Providers, by altering their liability for Internet content. A combination of all three approaches may also be attempted, as currently in France.

Within this framework, there is a choice of implementation methods. Legislation can mandate any of these methods, but as any such legislation would be controversial from a legal, economic and civil liberties perspective, few will take the heavy-booted route of the French government, and drive it through the legislature. Instead, some member state governments such as the UK, are seeking to by-pass the legislative scrutiny and push for so-called "voluntary" agreements between the Internet and the rights-holder industries. The courts may also be used to obtain orders for ISPs to supply information on users for civil sanctions, or to obtain filtering orders.

Graduated response outlined

At the centre of the policy debate is a set of proposals by the French government, known as graduated response. Graduated response has been developed in France as a legal response to the downloading of copyright protected content without payment or permission. It is frequently also known as '3-strikes', so-called because of the three levels of warning and penalty. Users who are alleged to have downloaded copyrighted content may be sent warning emails (strike one). If they do not change their behaviour, they will be sent a letter by recorded post (strike 2). If they still do not stop, their Internet access will be terminated for up to one year, and they

will be put on a blacklist, so that they cannot sign up with another Internet provider during that time (strike 3).

Graduated response – contract not copyright What is not well understood about graduated response is that it is grounded in contract law, not copyright law. This is one of legal work-arounds campaigned for by the rights-holders. For example, Shira Perlmutter, vice president of IFPI, the European recording industry association, speaking at a Westminster e-Forum: '*the concept is just that ISPs would implement the terms and conditions of their subscriber contracts once they have been notified that those terms and conditions have been breached and there has been an abuse of their service....So the concept is, if we, the rights holders, notify the ISP that a particular IP address is the source a major infringement, that should trigger some action by the ISP in enforcing of implementing those terms of service*"[xxiii].

The French law on 'Creation and Internet[xxiv]' does not directly sanction users for copyright infringement. Instead, it places on users an 'obligation to control their Internet access' and will sanction them for 'failure to control' where the 'failure' is evidenced by the downloading of copyright-infringing content. The mechanism for implementing this is the user's contract with their Internet service provider (ISP). The contract will have to state that users must control their Internet access together with the ISP's right to terminate. This helps us to understand the significance of the amendments related to user contracts and 'restrictions' in the Telecoms Package.

Network filtering as a policy option

Network filtering is an umbrella term that is often used to describe different techniques, which may include the blocking of websites or webpages. It is also used to describe techniques which block peer-to-peer transmissions to and from websites and servers.

Network filtering can be used as an alternative to physically cutting off Internet access to the home – in other words, it is an alternative to strike 3 of graduated response. Filtering provides an automated way to sanction users, simply by stopping or slowing users' connections mid-stream. Anyone spotted doing peer-to-peer downloading will find their connection suddenly slows down or stops completely[xxv].

Given that peer-to-peer traffic is the top target of the rights-holder industries, this makes it a very attractive option – at least from the viewpoint of member state governments who are under pressure from rights-holder industries, and who are also now aware of the political fall-out from a policy of cutting off users from the Internet. It is understood, for example, that the UK government is seriously considering peer-to-peer filtering in the discussions it is brokering between the two industries [xxvi].

However, filtering also raises some difficult issues from a policy viewpoint. Peer-to-peer blocking has been identified by the FCC in the US, as a discriminatory practice – discriminating against users according to the application they choose to use, is not acceptable (FCC Comcast order) .

Filtering and liability Another issue, highlighted by the management consultancy Booz and Company[xxvii], is the exposure of the ISPs to liability for over-blocking of content, or under-blocking . Users and web publishers may sue for content wrongly blocked. Rights-holders may sue for content not blocked.

Booz and Company also point out that filtering is technically difficult and entails high capital investment costs, and is so far not proven to work effectively. Their view is backed up by the verdict recently in a Belgian court in the case of Sabam versus Scarlet. In June 2007, Sabam obtained an order that Scarlet should filter content travelling across its network. It was asked to filter out and block transmissions of audio-files for which Sabam represents the copyright, using a technology supplied by Audible Magic. On 24 October 2007, Scarlet was released from the mandate, on the basis that the Audible Magic filtering technology did not work on its network[xxviii]

From discussions with vendors of filtering technology, it becomes evident that the technology can identify certain types of content and protocols as they travel down the network, but that the higher-level solutions demanded by the rights-holders will be either not possible, or will spoil the service to other users by slowing down the networks. The vendors say it *may* be possible to marry up their technology to a database such as Audible Magic to identify individual items of content, but were not convinced it would be cost-effective. However, they are clear that the technology cannot determine whether or not a user has a right to use that content, or whether it falls under any one of the legal exceptions under copyright law[xxix].

Finally, as Booz and Company[xxx] say, the public will tolerate a very limited amount of filtering for content which is universally agreed to be beyond the boundaries of acceptability – such as images of child sexual abuse – which is in any case illegal and dealt with by law enforcement officers. But there is no over-arching public support for filtering to support copyright.

Filtering, traffic shaping and quality of service However, policy on filtering becomes muddied because it is often confused with another technical function, namely network management. In fact, what they are really talking about is a double-edged sword. The same technology that facilitates facilitates monitoring and filtering also facilitates quite normal network management functions for ISPs, and in particular, something they refer to as traffic shaping.

Traffic shaping means that you manage the flow of data on the network so that everybody gets through in a fair manner – rather like you might try to manage the flow of vehicles on a motorway. You may slow down those that are going too fast, you may squeeze and re-shape anything that is taking up more than one lane, and you may alter the priority to let some vehicles through immediately and make others wait. ISPs say that traffic shaping is necessary in order to be fair to everyone, especially with the increasing amount of audio-visual, voice and gaming traffic. It's not fair if you can't hear properly on the telephone because your neighbour is downloading a film, so they make it right for you. This is also known in the industry as maintaining quality of service.

Traffic shaping is driven by rules which the ISPs enter into a database. It becomes filtering when the rules are altered – for example, instead of setting the rules to be fair to all, they deliberately re-set the rules to be unfair to some.

ISP liability and 'mere conduit'

Currently, the mere conduit principle, enshrined in the E-commerce directive, exonerates ISPs from any liability for the content they carry, as I have previously argued[xxxi]. They are 'mere conduits[xxxii]' – they are a transit system, and like the post office, they carry the traffic, but do not know or care what type of content is contained within the data packets[xxxiii] they transmit. There is a twin provision in the E-commerce directive, that governments shall not ask ISPs to monitor traffic[xxxiv]. These provisions have enabled ISPs to successfully argue that they cannot be asked to enforce copyright, when approached by rights-holders. Arguably, these provisions have also had the effect of protecting users freedoms[xxxv].

However, it is these very provisions which prompted the rights-holders to look for ways to amend the Telecoms Package. They sought a way to make the ISPs liable for content, they are put into a position of having to enforce it. Effectively, this would be about some form of secondary liability.

For example, the author's society GESAC, one of the groups which campaigned for the changes to the Telecoms Package, argued that the e-Commerce Directive (2000/31/EC) did not take account of the responsibility of the network operators, in cases where a customer infringed copyright. Veronique Desbrosses, GESAC secretary-general, is quoted as saying that including copyright in the Telecoms Package would show "a willingness to deal with the issue of copyrights and would constitute a starting point to work from."[xxxvi]

What has happened with the Telecoms Package, is a number of legal work-arounds. The provisions in the E-commerce directive remain in place, and it is understood that they will remain untouched for the foreseable future[xxxvii]. Therefore, the aim was to put pressure on that 'mere conduit' status, to somehow undermine it, and establish ways in which ISPs would have to accept liability for copyright infringement.

Policy implementation and the Telecoms Package

Having established the policy framework for copyright enforcement, it is now easier to see how it has been inserted in to the Telecoms Package.

Anchoring graduated response in the Telecoms Package

Graduated response has been anchored in to the Telecoms Package with Article 33 (2a) of the Universal Services Directive. This says that ISPs must "co-operate" with " the sectors interested in the promotion of lawful content". These sectors are clearly the rights-holder industries. MEP Ruth Hieronymi confirmed that the intent of this Article related to "Olivennes" measures[xxxviii]. . As I have argued in my previous papers, "co-operation" has been defined in the wider policy agenda as meaning graduated response and content filtering. [xxxix]

Article 33(2a) is linked from the pivotal Article 8 (4g) in the Framework directive. It establishes the concept of lawful content. It is pivotal because it is referenced in the Authorisation directive and the Access directive, thus it hooks in these key concepts for copyright enforcement at every level of the law.

End user contracts – the poisoned chalice Given that the mechanism for implementing graduated response is contract law, it then becomes obvious, why, in the Telecoms Package, the Universal Service directive had to be amended to impose new contractual requirements onto the ISPs. Specifically, the requirement to state any restrictions on access to content, services and applications, in the user contracts (Article 20(2)) Inclusion of these restrictions in the contract, gives the ISP the right to block users access to copyright protected content, and to terminate their contract if it catches them downloading copyright protected material. These amendments protect the liability of the ISP in the case where a user complained of a restriction or termination.

Thus apparently innocuous change lays a key foundation stone for a graduated response regime. And what has been touted as great news to users, may in fact, be a poisoned chalice.

Transparency – how a positive right could become negative Transparency is about keeping the user informed as to the terms and conditions of that ISPs service, and the requirement is similar to the requirement for the contract clauses, outlined above. In the Telecoms Package, transparency is taken to mean informing the user after the initial contract has been signed. It should be good for the user, because they will know exactly what they should be getting from their service provider, and this is how it was positioned. The Telecoms Package (Universal Service directive, Article 21 4(c)) requires ISPs to keep users up to date of any changes to the restrictions on access to 'lawful' content, services and applications, and backs up the ISP's contractual rights to block, restrict or terminate access.

The transparency requirement could potentially be quite a powerful user safeguard, especially when ISPs are also required to publicise their restriction criteria and keep the regulator informed (as they would with Universal Services directive, Article - 28 (2a)).

However, transparency, like contracts, may also be used to restrict the user's rights. Article 28 (2a) was dropped from the Council draft at the time of writing, with no explanation. And if ISPs are allowed to set restrictions without regulatory oversight, the transparency mechanism can be manipulated. ISPs could potentially use it to justify any restriction they choose to place onto users, such as forbidding peer-to-peer file sharing or blocking certain content. Thus, what should be a positive right for the user turns into a negative one – and perhaps, another poisoned chalice.

The Telecoms Package and network filtering

The Telecoms Package does not mandate filtering because to do so would contravene established principles of the E-commerce directive. When we seek to understand how the Telecoms Package might facilitate or open the scope for network filtering, we need to look at the amendments which deal with what in the Internet industry is known as network

management or traffic shaping. In examining the text of the Telecoms Package, we may also look for terms like degradation or restriction of service, and 'hindering' or slowing down of traffic, and quality of service (QoS).

However, there is a lot of doubt and uncertainty, even among the lawyers whom I have consulted, as to how the Telecoms Package really deals with filtering, and how certain amendments should be viewed. I have presented some views in the Annexe to this paper. One area of doubt is just how far it does give ISPs the opportunity to classify peer-to-peer file sharing as, for example, an activity which 'hinders' the availability of the network? Or, taking another example, classify it as 'unauthorised' traffic, and thus give them a mechanism to legally throttle or block peer-to-peer users - provided of course, that they put the particulars of the restriction in the user contract.

Another area that has been raised relates to the way the e-Privacy directive deals with the processing of traffic data. The German digital rights group, Arbeitskreis Vorratsdatenspeicherung (AK Vorrat)[xl] , claims that the directive opens up the processing of retained communications traffic data for the purposes of copyright enforcement – that is, archived records of Internet usage can be accessed and analysed by ISPs on behalf of rights-holders[xli]. Potentially, ISPs would need to do this to comply with graduated response requests from rights-holders, where access to users' web traffic records is essential in identifying the subscriber as an individual[xlii].

It is evident though, that there is an attempt to make the regulation of this area as loose as possible, and the changes in the Presidency compromise proposals make it even looser than the Parliament's version. Given what we know of the policy framework and the wider agenda, we can expect to see filtering of content in various forms coming in, if the Telecoms Package is passed as it stands - unless the relevant provisions are either removed to make way for further consultation or amended to be more clear as to the intent, the filtering criteria and the triggers for regulators to intervene.

Protecting lawful content and ISP liability

The Telecoms package imposes on the national regulators, a requirement to promote 'lawful' content, and to promote 'co-operation' between ISPs and '*the sectors interested in the promotion of lawful content*' (that is, the rights-holders). The word 'promote' is, in this context, a powerful word, since it is also used in the context of 'promoting competition' among telecoms operators – competition is a key policy in the telecoms market. If 'promoting' competition is important, then presumably 'promoting co-operation' is too.

Lawful content But what is 'lawful content'? This is a new concept of lawful content in European law, introduced in the Telecoms Package.

The easiest way to understand it, is to consider the distinction between "unlawful" and "illegal". Illegal means that it breaks a law – and child pornography[xliii] and certain forms of hate speech fall into this category. "Unlawful" means that it violates a statutory requirement.

Thus unlawful content could be considered as content which violates copyright. It isn't the content itself which is unlawful, but the act of reproducing it in a digital file, or making it available to other file-sharers, without payment to or permission from, the rights-holder, or any other exception to copyright law applying – it therefore breaches copyright law and means that it is unlawful.

Thus, the only meaningful way to interpret it is that protecting 'lawful' content is protecting content which does not violate copyright. It is furthermore evident that the only lawful content that will receive any protection is that which commercially valuable, and either owned by one of the large media companies, or represented by one of the collecting societies.

Or to put it simply, Disney's *Snow White* will be protected. A film by a student film producer, will not, even though it may not violate any copyrights. Similarly the vast volume of other content, software applications and website services which breaches no rights and breaks no law, will receive no protection.

Lawful content and liability The question is how far the Telecoms Package goes towards obligating ISPs to enforce lawful content, and therefore, how far it pushes them on the liability issue. At what point would they start filtering and blocking to protect themselves from secondary liabilty lawsuits? A view has even been expressed that there is a presumption that all content is unlawful until filtered[xliv] . Put differently, the text[xlv]' restricts users access to 'lawful' content, and thus it closes the pincers on the ISPs to enforce copyright.

As we have seen, filtering could leave them heavily exposed. It is impossible for an automated filter to distinguish whether a user has a right to use content. Over-blocking exposes them to liability for blocking content which is legitimate and legal and does not breach any rights. Conversely, the ability of users to find work-arounds, and circumvent the filters, exposes them to secondary liability actions from the rights-holders[xlvi].

Filtering also has the effect of slowing down the network. How much it slows down, depends on the scale of the filtering. But if the filtering demanded by rights-holders were to noticeably slow the download speeds for a majority of users, that would expose the ISP in terms of meeting any quality of service obligations – which may also be in the user's contract.

Would ISPs be entitled to restrict users to copyright-protected content only - a scenario which would result in ISPs becoming more like a broadcast network, and users without access to the public Internet. What is the regulatory trigger which enables regulators to intervene in cases of unlawful filtering?

Safeguards for users

Copyright enforcement policy raises a range of civil liberties issues. For example, the potential for users to be sanctioned by private enforcement methods, and to receive summary justice by abrupt disconnection mid-transmission, without the right to defence. From a policy perspective it is important to consider how to safeguard users against abusive tactics by rights-holders or network operators.

As voted by the European Parliament, the Telecoms Package incorporates some safeguards. They have been removed in the European Council's draft compromise proposals, at the time of writing.

Proportionality and due process

The European Parliament voted in two key amendments, designed to protect users from excessive or unreasonable sanctions. The Universal Service directive Article 32a – also known as the Harbour report Amendment 166 - would mean that any action to restrict access to content, services and applications would have to be proportionate and applied in a fair manner with due process. Thus, it sets up a series of legal tests, which governments and regulators would have to comply with in setting up any kind of graduated response mechanism. This would also appear to preclude the use of automated filtering techniques to block peer-to-peer users, where by the nature of the sanction, there is no due process.

The Framework directive, Article 8 (4ga) - also known as Trautmann report Amendment 138 - would mean that any sanctions have to be subject to a court order or judicial oversight. It says that you can't have a system where rights-holders basically tell the ISPs 'this person is a repeat infringer' and the ISP will implement the contract and cut them off, without any form of due process – in other words, a court . The French proposal to have a public authority, is little more than window-dressing – done for show - as the authority will act on the basis of information provided by agents, who are in fact the collecting societies and rights-holder associations.

The Council of Ministers draft proposals had dropped both amendments, at the time of writing, which, unless they were reinstated, would open the scope for termination or other sanctions.

Regulatory oversight and accountability

What is missing from the entire Telecoms Package, is any notion of accountability for blocking access to content and punishing users. Under both the UK and the French proposals, the rights-holders will be sole arbiters of what is and isn't lawful – and thus, they will be in a position to determine what users may or may not access on the Internet. Rights-holders are private corporations with vested interests in promoting *their own* content.

The *lawful content* limitation in the Telecoms Package misses an important point concerning the protection of users rights to access public domain content on the open Internet. What regulation is there to deal with rights-holders and ISPs teaming up to provide bespoke services, which block users from the open Internet and public domain content? Should a duty be imposed upon regulators to protect users access to the open Internet and public domain content, in an environment where rights-holders and ISPs jointly control content access?

Given the complexities of EU copyright law, it is also essential for there to be a transparent dispute mechanism where users can raise objections to sanctions. The Telecoms Package, whilst setting up the framework as per the rights-holders demands, leaves out this crucial

mechanism for users' defence against unfair or unwarranted allegations. There are no dispute resolution mechanisms, which is also a failing raised in the French Senate on 31 October when it debated the Creation and Internet law. [xlvii]

Filtering – whether throttling or blocking – raises special issues. It implies an automated sanction, applied surreptitiously, without necessarily even notifying the user. Blocking of peer-to-peer content is a random and unspecific technique, which blocks all users of a particular technical application. It takes no account of whether they are copyright infringing, or transferring content which has nothing to do with copyright matters – for example, software which they are working on[xlviii]. It is done on the assumption that a "majority" of peer-to-peer traffic infringes copyright. Even that phrasing leaves room for a "minority" that does not infringe and has a right to carry on connecting. Blocking peer-to-peer traffic has been called disriminatory because it discriminates against people who choose peer-to-peer instead of YouTube.[xlix]

Filtering also raises privacy issues. The deep packet inspection methods used to block peer-to-peer connections at an individual level are technically interception[l] and in this respect violate privacy rights. Privacy concerns are also raised by the possibility of retaining web traffic data for the purposes of assisting rights holders in identifying users who are alleged to have infringed copyright. Will it be the case that all of our web surfing records – every website we visit – would have to be stored, just in case we were accused under a graduated response or "co-operation" scheme?

The powers of oversight for both national regulators and the European Commission, are therefore essential in maintaining an equitable access for all users. The amendments to the Telecoms Package weaken the ability of regulators and the European Commission to intervene in cases of filtering content, traffic shaping, or graduated response. The only possible safeguard has to come via the regulator who has a duty to oversee both industries on behalf of citizens.

Where we are placing new restrictions onto users, and we know that those restrictions relate to the requirements of a third party industry. We must also offer safeguards for users and we must be clear whether and why and how , if at all, those restrictions may be imposed outside the usual legal structures.

---

[i] Presidency compromise proposals to Council Working Party on Telecommunications and Information Society – see list of documents in the Annexe to this paper.
[ii] Viviane Reding, European Commissioner for Information Society, letter to Jean-Paul Salome, president of the ARP, dated 8 October 2008
[iii] See Annexe, page 1
[iv] European Data Protection Supervisor's report, 2 September 2008 p12
[v] Evi Werkers and Fanny Coudert, The fight against piracy in peer-to-peer networks: the sword of Damocles hanging over the ISP's head? Paper submitted for the 17th International Conference on Information Systems Development (ISD 2008), Paphos, Cyprus, 25-27 August 2008 , p3
[vi] Peer-to-peer technologies in fact up-and-download at the same time, however, I am using the term 'downloading' as this is what is commonly understood.
[vii] IFPI submission to the European Commission, Creative Content Online consultation, 29 February 2008, p 14

[viii] I am referring here to documented rights-holder lobbying in fora which include: European Commission Creative Content Online consultation, Westminster e-Forum(see viii below), ACTA negotiations, Mission Olivennes consultation, European Parliament –Telecoms Package, Bono report.
[ix] Shira Perlmutter, legal counsel for IFPI, speaking at Westminster e-Forum, Intellectual Property and the Future of Copyright, 31 March 2008, p 24 of transcript.
[x] The could of course, advertise,. but that is indirect communication.
[xi] Motion Picture Association (MPA) submission to European Commission Content Online consultation, October 2006 and February 2008.
[xii] Directive 2001/29/EC on on the harmonisation of certain aspects of copyright and related rights in the information society
[xiii] Directive 2004/48/EC
[xiv] Consultation for Creative Content Online, commenced July 2006, still ongoing
[xv] Report on the Cultural Industries in Europe, Committee on Culture and Education. Rapporteur: Guy Bono. A6-0063/2008
[xvi] Amendment 80, Paragraph 9a new, by Christopher Heaton-Harris, (UK,Conservative). PE 398.378v01-00
[xvii] Bruxelles entend faire respecter le droit d'auteur dans les télécoms, 31 October 2007, Les Echos, Karl de Meyer
[xviii] MEP Ruth Hieronymi, speaking at a French embassy seminar in Berlin, "Kann die Olivennes-Vereinbarung die Weichen für die digitale Zukunft stellen?" 15 October 2008. Recorded by Netzpolitik. http://asset.netzpolitik.org/wp-upload/ruth_hieronymi_urheberrecht.mp3
[xix] ibid European Data Protection Supervisor, p12
[xx] Liberation.fr, Un front européen contre l'amendement 138 ? http://www.ecrans.fr/Un-front-europeen-contre-l,5611.html
[xxi] There is a fourth approach using criminal sanctions, as in the IPRED2 directive and also discussed within the ACTA Anti-counterfeiting trade agreement, but this is outside the scope of this paper.
[xxii] Booz and Company, Digital Confidence, Securing the next wave of digital growth, Liberty Global Policy Series, (2008) p67, column 2. The UK government is considering this option.
[xxiii] Shira Perlmutter, executive vice president, IFPI, speaking at Westminster e-Forum, 31 March 2008
[xxiv] Le projet de loi favorisant la diffusion et la protection de la création sur Internet
[xxv] The most effective way to block peer-to-peer transmissions is technically known as TCP packet reset, which involves the ISP pretending to the user, that the other computer has stopped transmitting, causing the users computer to stop.
[xxvi] ibid Booz and Company, p67
[xxvii] ibid Booz and Company, pp64-66
[xxviii] Sabam v Scarlet, Tribunal de Premiere Instance Bruxelles, 22.10.2008
[xxix] Meetings with Dave Caputo, CEO, Sandvine, and representatives of Procera, Cisco and Nortel, at the Broadband World Forum, Brussels, 1 October 2008.
[xxx] ibid Booz and Company, p64
[xxxi] *The 'Telecoms Package' and the copyright amendments – a European legal framework to stop downloading, and monitor the Internet*. Monica Horten, 30 June 2008. Available on www.iptegrity.com
[xxxii] Directive 2000/31/EC, Article 12.
[xxxiii] Packets – data on the Internet travels in packets, and the technique is known as packet switching.
[xxxiv] Directive 2000/31/EC, Article 15.
[xxxv] ibid Evi Werkers and Fanny Coudert, p3
[xxxvi] Telecoms package will impose respect of copyrights, 2 November 2007, Europolitics
[xxxvii] Reuters, 24 June 2008, 6.15 pm, No need to update EU's e-commerce rules-McCreevy
[xxxviii] ibid, MEP Ruth Hieronymi
[xxxix] Monica Horten, The 'Telecoms Package' and the copyright amendments – a European legal framework to stop downloading, and monitor the Internet, 30 June 2008
[xl] AK Vorrat, Position on the processing of traffic data for "security purposes" , 4 November 2008
[xli] Web traffic data was explicitly excluded from the Data Retention directive (2006/24/EC), as was access to retained data for copyright enforcement purposes
[xlii] Creative and Media Business Alliance (CMBA), Position on Data Retention, 22 November 2005.

[xliii] Child pornography falls under the child abuse and sexual offenders legislation.
[xliv] Business Software Alliance (BSA) News release: Review of European telecommunications laws, BSA calls on the Council of the European Union to ensure the security of online users without enacting unworkable requirements affecting the processing of Internet traffic data and warns against the imposition of anti-piracy filtering technologies Brussels, 24 September 2008
[xlv] Article 8 (4g) of the Framework directive – see Annexe to this paper
[xlvi] ibid booz and Company, pp64-65
[xlvii] Video stream of the proceedings in the French Senate on 30 October, at the time available at http://www.ecrans.fr/Direct-le-debat-sur-la-riposte,5564.html via the Senate's own web streaming service, Public Senat. Senators debated the need for a hotline, as a minimum, for users to call on receipt of a warning email.
[xlviii] When throttling, the ISP will looks for specific peer-to-peer protocols, for example Bit Torrent, and slow down all those users. It does not look any deeper into the content. This can be done, in theory, but in practice has so far proved not to work (ref. Sabam v Scarlet, Tribunal de Premier Instance, Brussels, 27 October 2008).
[xlix] FCC Comcast order, 20 August 2008
[l] Reponse de l'AFA a la consultation de la Commission Europeenne sur les contenus creatifs en ligne dans le marche unique , 29 February 2008, p15